

CalSAWS PRIVACY AND SECURITY AWARENESS TRAINING

INTRODUCTION

Training is designed to provide users of the CalSAWS system the knowledge to protect information systems and sensitive data from internal and external threats. This course fulfills the Privacy and Security Agreement flow down policies for safeguarding data required by the Social Security Administration, the Federal Information Security Management Act of 2002 (FISMA) and the Consumer Privacy Protection Act of 2017.

TRAINING FORMAT AND SECTIONS

- I. Federal and State Laws
- II. Flow Down Regulations
- III. PII and PI
- IV. Other Important Regulations and Standards
- V. Safeguarding Privacy Data
- VI. Security Breach and Data Loss Incident Reporting Procedures
- VII. Threats to Access Control
- VIII. Sanctions Policy for Privacy and Security Violations

TRAINING GOALS AND OBJECTIVES

Goal #1 : Facilitate Understanding of Federal and State Laws, Executive Orders, Directives, Government Policies and Regulations applicable to the CalSAWS Program.

OBJECTIVES

- # 1: Introduce users to the Consumer Privacy Protection Act of 2017 and how it relates to the CalSAWS Program.
- # 2: Introduce users to the Health Insurance Portability and Accountability Act of 1996 (found in 45 CFR 160 and 164).
- # 3: Introduce users to the Social Security Administration (SSA) “Security Awareness Training, Employee and End User Sanctions Policy and Incident Response Policy”.
- # 4: Introduce users to the California Consumer Privacy Act (CCPA)

Goal #2: Achieve Compliance with CalSAWS Privacy and Security Agreements (PSA's)

OBJECTIVES

- # 1: Ensure users understand the flow down requirements as a result of the executed PSA's between CalSAWS and the Department of Social Services (CDSS) and CalSAWS and the Department of Healthcare Services (DHCS).
- # 2: Ensure users understand and acknowledge their responsibilities when accessing the CalSAWS System.

Goal #3: Facilitate Compliance with CalSAWS Policies and Best Practices

OBJECTIVES

- # 1: Provide users with an overview of Information and Privacy and Security best practices and standards described in NIST Special Publication (SP) 800-53r4 as they relate to the CalSAWS Program.
- # 2. Introduce users to the CalSAWS Program Security Requirements and Security Controls based on NIST SP 800-53r4.
- # 3: Train users on Rules of Behavior and their Responsibilities while accessing the CalSAWS system.

TRAINING GOALS AND OBJECTIVES - CONTINUED

Goal #4 : Achieve Code of Federal Regulations Compliance for Information Systems Security Awareness Training

OBJECTIVES

- # 1: Establish and provide annual privacy and security awareness training to CalSAWS users.
- # 2: Develop and implement metrics to track the progress of the privacy and security awareness training.
- # 3: Ensure users of the system understand their responsibility in protecting and safeguarding CalSAWS information.

Goal #5: Reduce Security Threats

OBJECTIVES

- # 1: Raise user awareness by providing rules of behavior and use case scenarios in training materials.
- # 2: Provide users with a mechanism to report, inquire and discuss privacy and/or security concerns.
- # 3: Describe the common threats to access control and the countermeasures that users must practice to protect CalSAWS environments and information.

Goal #6: Mitigating Risks from Security Incidents

OBJECTIVES

- # 1: Share the process on responding to security incidents so handling of incidents are effective and efficient.
- # 2: Provide users with a mechanism to report, inquire and discuss privacy and/or security concerns.
- # 3: Describe the common threats to access control and the countermeasures that users must practice to protect CalSAWS environments and information.

FEDERAL AND STATE LAWS

Several Federal and State Laws mandate protection of consumer data.

The Consumer Privacy Protection Act of 2017, “Ensures the privacy and security of sensitive personal information, to prevent and mitigate identity theft, to provide notice of security breaches involving sensitive personal information, and to enhance law enforcement assistance and other protections against security breaches, fraudulent access, and misuse of personal information”.

The Health Insurance Portability and Accountability Act of 1996 provides data privacy and security provisions for safeguarding medical information in the United States.

The California Consumer Privacy Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of the state of California.

The Computer Matching and Privacy Protection Act of 1988 (CMPPA) requires Federal agencies to enter into written agreements with other agencies or non-Federal entities before disclosing records for use in computer matching programs. And specifies areas to be addressed in such agreements, including justification for matching, notifying individuals (including Federal employees) whose records are to be matched, procedures for retention and destruction of data after matching, and prohibitions on disclosure of records and the compilation of data.

SECTION III

PRIVACY SECURITY AGREEMENTS AND FLOW DOWN REGULATIONS

PRIVACY SECURITY AGREEMENTS (PSAs) AND FLOW DOWN REGULATIONS

Training includes flow down regulations from the Privacy and Security Agreements (PSAs) between The Department of Health Care Services (DHCS) and the California Department of Social Services (CDSS) to the California Statewide Automated Welfare System Joint Powers Authority (CalSAWS Consortium). Inherited flow down regulations stem from the Social Security Administration (SSA), the Employment Development Department (EDD) and the Department of Homeland Security (DHS).

FLOW DOWN REGULATIONS APPLICABILITY

SSA requires CalSAWS to certify that each employee, contractor and agent who views SSA-provided information certify that they understand the potential criminal, civil and administrative sanctions or penalties for unlawful access and/or disclosure.

Federal and State laws require that security and privacy awareness and sanctions be formally communicated and acknowledged by consortium employees, vendors, contractors and sub-contractors (herein referred to as individual or workforce) accessing CalSAWS information (herein referred to as information) and CalSAWS data (herein referred to as data).

SSA flow down regulations applicable to the CalSAWS workforce include “Security Awareness Training, Employee and End User Sanctions Policy and Incident Response Policy”.

CalSAWS SYSTEM, MISSION AND CORE PROGRAMS

As per the California Assembly Bill 1811 as chaptered by the Secretary of State on June 27, 2018, Sec. 15, The Legislature finds and declares all for the following:

1. Through the Statewide Automated Welfare System (CalSAWS) consortium, the state and counties provide health and human services to over 13 million Californians.
2. The state is currently working in partnership with the federal government to consolidate the existing consortium systems and functionality into one single California Statewide Automated Welfare System (CalSAWS). This consolidation will heavily leverage the existing Los Angeles Eligibility, Automated Determination, Evaluation, and Reporting (LEADER) Replacement System, rather than building a new system.

3. California, its counties, and stakeholders have decades-long partnership and commitment to excellence in service delivery for its health and human services programs. This partnership is a relationship built on effective communication, transparency, and a shared vision of service to millions of low-income and vulnerable Californians.
4. The CalSAWS will be the primary automation system for delivering benefits for several decades.
5. The CalSAWS development process will be improved through meaningful stakeholder, client and advocate input on elements that impact service delivery.

The CalSAWS System is the county-administered automated case management system that supports California's public assistance programs with the automation of county welfare business processes in California. These business processes support eligibility determination, benefit computation, benefit delivery, case management and information management.

The approach currently includes three county-level consortia welfare systems and a state-level database to track (1) Temporary Assistance to Needy Families (TANF), (2) California Work Opportunity and (3) Responsibility to Kids (CalWORKs) time on aid.

CORE PROGRAMS

The CalSAWS system supports six core programs and many sub-programs. The core programs are:

1. CalWORKs
2. SNAP (known as CalFresh in California)
3. Medicaid (known as Medi-Cal in California)
4. Foster Care
5. Refugee Assistance
6. And County Medical Services

CalSAWS PRIVACY SECURITY AGREEMENTS

TERMS, CONDITIONS AND SAFEGUARDS

CalSAWS receives this data through the Information Exchange Agreement (IEA) in the PSA. The IEA establishes terms, conditions and safeguards under which these external federal systems will disclose certain information, records and data.

The Electronic Information Exchange Security (EIES) Requirements mandate that CalSAWS provide copies of the agreement to vendors and all related attachments before disclosure of data. CalSAWS is required to maintain a list of individuals who access the CalSAWS data. And CalSAWS must provide proof of the contractual agreement with all vendors. The EIES mandates Security and Privacy Awareness Training and Proof of Security Controls.

NON-DISCLOSURE AND ATTESTATION REQUIREMENTS

The non-disclosure attestation must also include acknowledgement from each individual of the workforce that he or she understands and accepts the potential criminal and/or civil sanctions, or penalties associated with misuse or unauthorized disclosure of program provided information or data.

The CalSAWS Consortium must retain the non-disclosure attestations for minimum of (5) years, or a maximum of seven (7) years for everyone who processes, views or encounters SSA-provided information as part of their duties.

CalSAWS CONSORTIUM REQUIREMENTS

The CalSAWS Information Security and Privacy Office Responsibilities

1. Ensure the delivery of this training to the workforce annually.
2. Certify that the workforce acknowledges that they understand the potential criminal, civil and administrative sanctions and penalties as described in this training for inappropriate, intentional, unintentional or unauthorized use of CalSAWS information and data.
3. Administer and Track workforce training and completion of non-disclosure agreements training.
4. Proof of contractual agreements with all vendors and written certification that the contractor is meeting the terms of the PSA and IEE Agreements.
5. Make training information available to oversight auditors.

WORKFORCE REQUIREMENTS

Must complete this training and sign the PSA required non-disclosure agreement to attest to the following:

1. You have received the mandatory security and privacy awareness training
2. The program rules of behavior have been explained to you
3. You understand the program security controls and privacy safeguards for information and data through the use of the CalSAWS system
4. You understand the sanctions
5. You have been provided information for communicating concerns regarding this training and the required non-disclosure agreement.

THE SOCIAL SECURITY ADMINISTRATION

WHAT IS SSA DATA?

“SSA Data” means information under the control of SSA provided to an external entity under the terms of an information exchange agreement (IEA) with SSA.

“SSA Data” also includes information provided to the Electronic Information Exchange Partner (EIEP) by a source other than SSA, but which the EIEP:

- Attests to that SSA verified it, or
- The EIEP couples the information with data from SSA to certify the accuracy of the information.

THE TWO FORMS OF SSA DATA IN CalSAWS

Data provided

- SSA provided date of death;
- SSA Title II (Disability Insurance Program) benefit and eligibility data;
- SSA Title XVI (Supplemental Security Income (SSI) Program) benefit and eligibility data;
- SSA Citizenship verification.

Data verified by SSA and evidence of the verification

- SSN and associated SSA verification indicator displayed together on a screen, file, or report; or
- DOB and associated SSA verification indicator displayed together on a screen, file, or report.

EXAMPLES OF SSA DATA

- SSA's response to a request from an EIEP for information from SSA (e.g., date of death)
- SSA's response to a query from an EIEP for verification of an SSN
- Display by the EIEP of SSA's response to a query for verification of an SSN and the associated SSN provided by SSA
- Display by the EIEP of SSA's response to a query for verification of an SSN and the associated SSN provided to the EIEP by a source other than SSA
- Electronic records that contain only SSA's response to a query for verification of an SSN and the associated SSN whether provided to the EIEP by SSA or a source other than SSA

SSA DATA IN THE CalSAWS SYSTEM

The CalSAWS system utilizes data and information from DHS, EDD and SSA (here in referred to as external federal systems) through DHCS and CDSS interfaces to determine entitlement and eligibility for individuals for one or more of the statewide county programs in the state of California. CalSAWS also sends batch files to external federal systems through these interfaces.

CDSS provides data received from Department of Homeland Security SAVE program which provides immigration status information from federal immigration records. This information is used to verify immigration status to non-U.S. citizens who apply for federal benefits under TANF and SNAP programs.

DHCS provides SSA data in order to administer state-funded benefit programs. The use of this data expedites the application process and ensures that benefits are awarded only to applicants that satisfy the program criteria. CalSAWS receives this information via the MEDS interface.

EDD offers a wide variety of services to millions of Californians under Unemployment Insurance (UI), State Disability Insurance (SDI), workforce investment (Jobs and Training), and Labor Market Information programs. CalSAWS receives UI and SDI information via the IEVS interface.

PROTECTING SSA DATA

- In addition to the federal and state laws discussed in this training, SSA data is also protected by the Privacy Act of 1974 (5 U.S.C. § 552a). This Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of record by federal agencies.
- The Consortium must adhere to specific privacy and information security requirements when working with SSA data. It is extremely important to remain compliant with SSA requirements in order to maintain access to SSA data.

ACCESSING SSA DATA

- ¹ SSA data is considered PII and access to it should be restricted to only those individuals authorized to access the data to perform their official duties as it relates to the CalSAWS program.
- Individuals include Consortium employees, contractors and vendors.
- The Consortium is required to provide all vendors and contractors copies of the Privacy and Security Agreements (PSAs) and related Information Exchange Agreements (IEAs), and all related attachments before initial disclosure of SSA data.

USE AND DISCLOSURE OF SSA DATA

Like PHI/PI, use and disclosure of SSA data is limited to purposes directly related to the administration of the CalSAWS Program:

- Determining eligibility
- Providing services to recipients
- Conducting or assisting in investigations, prosecutions or proceedings related to CalSAWS Programs
- Third party liability activities
- Audits and legislative investigations.

When providing SSA data to an outside entity, the Information Exchange Agreement (SSA Agreement) between DHCS and SSA must be attached to, and incorporated within, the data sharing or other applicable agreement.

DHCS and CDSS have entered into Privacy Security Agreements with CalSAWS. All CalSAWS vendor contracts must have the PSA amended into their contract in order for CalSAWS to be compliant with the PSAs.

SSA DATA – ACCEPTABLE USE

We will:

- Use and access SSA data only for verifying eligibility for benefit programs identified in the IEA.
- Only use Federal Tax Information (FTI) to determine eligibility for programs.
- Use citizenship status data only to determine entitlement of new applicants.
- Restrict access to SSA data to only those authorized State employees, contractors, and agents who need such data to perform their official duties.

SSA DATA – NOT PERMITTED

We will not:

- Use or redisclose SSA data for any purpose other than to determine eligibility.
- Extract information concerning individuals who are not applicants for, nor recipients of, benefits programs identified in this Agreement.
- Disclose to an applicant/recipient information about another individual without the written consent from that individual.
- Duplicate or disseminate SSA data without prior written permission from SSA.

Employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by this Agreement may be subject to civil and criminal sanctions pursuant to applicable Federal statutes.

INDIVIDUAL RESPONSIBILITY

When accessing SSA data, Consortium employees, contractors, and agents are responsible for ensuring its proper use and protection by:

- Adhering to all administrative, physical, and technical safeguards described in this training when working with SSA data.
- Viewing or copying only relevant parts of SSA data, when needed.
- Deleting, destroying, or purging any files, screen shots or print-outs containing SSA data when they are no longer needed for the intended business purpose.

SECTION III

PERSONAL INFORMATION (PI)
AND
PERSONALLY IDENTIFIABLE INFORMATION (PII)

THE PRIVACY ACT OF 1974

The Privacy Act of 1974 establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.

The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register.

The Privacy Act prohibits the disclosure of information from a system of records absent of the written consent of the subject individual, unless the disclosure is pursuant to one of twelve statutory exceptions.

The Act also provides individuals with a means by which to seek access to and amendment of their records and sets forth various agency record-keeping requirements.

Additionally, with people granted the right to review what was documented with their name, they are also able to find out if the "records have been disclosed".. and are also given the rights to make corrections.

Users of the CalSAWS system are expected to comply with limitations on use, treatment and safeguarding of data under the Privacy Act of 1974.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

The California Consumer Privacy Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States. The bill was passed by the California State Legislature and signed into law by Jerry Brown, Governor of California, on June 28, 2018, to amend Part 4 of Division 3 of the California Civil Code.

The intentions of the Act are to provide California residents with the right to:

- Know what personal data is being collected about them.
- Know whether their personal data is sold or disclosed and to whom.
- Say no to the sale of personal data.
- Access their personal data.
- Request a business to delete any personal information about a consumer collected from that consumer.
- Not be discriminated against for exercising their privacy rights.

WHO IS COVERED?

California residents who provide information such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers to applicable businesses.

CCPA defines personal information as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

An additional caveat identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, their name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

The following sanctions and remedies can be imposed:

- Companies, activists, associations, and others can be authorized to exercise opt-out rights on behalf of California residents (Cal. Civ. Code § 1798.135(c)).[5]
- Companies that become victims of data theft or other data security breaches can be ordered in civil class action lawsuits to pay statutory damages between \$100 to \$750 per California resident and incident, or actual damages, whichever is greater, and any other relief a court deems proper, subject to an option of the California Attorney General's Office to prosecute the company instead of allowing civil suits to be brought against it (Cal. Civ. Code § 1798.150).[5]
- A fine up to \$7,500 for each intentional violation and \$2,500 for each unintentional violation (Cal. Civ. Code § 1798.155).
- Privacy notices must be accessible and have alternative format access clearly called out.

RULES OF BEHAVIOR

HANDLING PERSONAL INFORMATION

Personnel shall comply with the provisions of Section 10850 and 18909 of the Welfare and Institutions Code, Division 19 of the California Department of Social Services Manual of Policies and Procedures, and all other statutory laws relating to privacy and confidentiality.” The referenced Welfare and Institutions codes stipulate that the data is confidential and shall not be disclosed.

In order understand the definition of data, the California Civil Code applies. As defined in California Civil Code section 1798.82, “any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

RESPONSIBILITIES UNDER THE PRIVACY ACT

Personal Information may not be printed, faxed, emailed, or stored on a laptop. Personal Information may not be taken from the CalSAWS project. Exceptions to this must be authorized by Project Executive Management.

Personal Information may not be printed, faxed, emailed, or stored on a laptop. Personal Information may not be taken from the CalSAWS project. Exceptions to this must be authorized by Project Executive Management.

EMAIL RESPONSIBILITIES

Some Personnel may retain email accounts provided by their employer's (vendor or county). Such accounts are important for conducting confidential business and personnel matters. The Consortium manages and administers the CalSAWS.org email accounts to conduct project business.

Personnel shall utilize their CalSAWS email accounts to conduct CalSAWS-related business. Exceptions to the use of the CalSAWS email domain include the following:

- Non-Project communications
- Confidential personnel matters

EMAIL ATTACHMENTS AND SPAM

Personnel must use caution when opening email attachments received from unknown senders, as they may contain viruses, worms, or Trojan horse code. Personnel should also be cautious of email from known individuals if the email subject or contents seem out of character for that individual. In such a case, Personnel should contact the sender and verify the validity of the email before opening it whenever possible.

Personnel must never reply to spam or take actions as requested in the message, such as clicking on a link, doing what it says about a virus, replying, or asking to be removed. from the mailing list. “Unsubscribing” from unsolicited spam messages typically serves to alert the sender that a valid email address exists and will generally result in even more spam being sent. Spam messages should be disregarded and promptly deleted. Personnel should also notify technical support if the spam becomes a nuisance.

Personnel must immediately open and act on any security message sent by CalSAWS Technical Support. Failure to do so can result in system compromise or data disclosure.

Unless it is received from CalSAWS Technical Support, Personnel must never take any action regarding virus notifications. Furthermore, Personnel must always let CalSAWS Technical Support handle communication to the project, remediation, and prevention.

Personnel are advised that many publicly distributed emails containing virus warnings are hoaxes and following such emails can result in computer damage.

Freedom of Information Act (FOIA)

Personnel must be aware that written communications may be subject to public disclosure pursuant to federal and state law, specifically the Freedom of Information Act (FOIA) and the California Public Records Act (CPRA). The CPRA was enacted in 1968 and codified as California Government Code § 6250 through § 6276.48. The fundamental precept of the CPRA is that government records shall be disclosed to the public, upon request, unless legally exempt from such disclosure or the public interest in nondisclosure clearly outweighs the public interest in disclosure.

Some exemptions to public disclosure include:

- Preliminary drafts, notes, or memoranda that are not retained by the public agency in the ordinary course of business
- Personnel, medical records, or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy
- Applications or records concerning any individual in connection with any form of public social services under the California Welfare & Institutions Code §10850
- Deliberative processes, discussions, or negotiations
- Trade secrets or proprietary information
- Attorney-client privileged communications
- Records pertaining to pending litigation to which the agency is a party, or to claims, until the litigation or claim has been finally adjudicated or otherwise settled

OTHER SECURITY RESPONSIBILITIES

Personnel are responsible for the following to help maintain CalSAWS system security:

- Personnel are prohibited from conducting unauthorized port or vulnerability scans or executing any form of unauthorized network monitoring.
- Personnel must not tamper with or circumvent user authentication or security of any host, network, or account.
- Personnel must maintain virus scanning utilities, personal firewalls, or other programs designed to protect systems, users, or information in good working order, with approved configurations intact.
- Personnel may not disable or modify any legal notice or warning banners on CalSAWS systems.
- Personnel may not tamper with or circumvent installed physical facility security measures.
- Personnel must safeguard Sensitive Information about security designs or implementations to prevent access by unauthorized persons.

SECTION IV

OTHER IMPORTANT REGULATIONS AND STANDARDS

OTHER IMPORTANT REGULATIONS AND STANDARDS

- ¹ The E-Government Act of 2002 established a new Office of Electronic Government within the Office of Management and Budget.
- ² NIST (National Institute of Standards and Technology) Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”:
 - Control Family “AT”, Awareness and Training
 - Control Family “PS” Personnel Security
 - Control Family “PM”, Program Management

¹ "E-Government Act of 2002", US Government Publishing Office (GPO), 17 Dec 2002, [https://www.govinfo.gov/E-Government Act of 2002](https://www.govinfo.gov/E-Government%20Act%20of%202002)

² "NIST Special Publication 800-53, Rev 4", National Institute of Standards and Technology (NIST), 22 Jan 2015, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>

¹ E-Government Act of 2002

The E-Government Act of 2002 (Pub.L. 107–347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803), is a United States statute enacted on December 17, 2002, with an effective date for most provisions of April 17, 2003. Its stated purpose is to improve the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a framework of measures that require using Internet-based information technology to improve citizen access to government information and services, and for other purposes.

¹ "E-Government Act of 2002", US Government Publishing Office (GPO), 17 Dec 2002, https://www.govinfo.gov/E-Government_Act_of_2002

AT-1, SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES:

- The organization develops, documents, and disseminates a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- The organization develops procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
- The organization reviews and updates the current security awareness and training policy and security awareness and training procedures.

AT-2, SECURITY AWARENESS TRAINING:

- The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial onboarding, when required by system changes, and on an on-going basis.

¹ "NIST Special Publication 800-53, Rev 4", National Institute of Standards and Technology (NIST), 22 Jan 2015, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>

...NIST 800-53: Awareness and Training (AT)

AT-3, ROLE-BASED SECURITY TRAINING:

- The organization provides role-based security training to personnel with assigned security roles and responsibilities as part of initial onboarding, when required by system changes, and on an on-going basis.

AT-4, SECURITY TRAINING RECORDS:

- The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training and retains individual training records for a specified period.

¹ "NIST Special Publication 800-53, Rev 4", National Institute of Standards and Technology (NIST), 22 Jan 2015, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>

NIST 800-53: Personnel Security (PS)...

PS-1, PERSONNEL SECURITY:

- The organization develops, documents, and disseminates a personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- The organization develops, documents, and disseminates procedures to facilitate the implementation of the personnel security policy.
- The organization reviews and updates the current personnel security policy and personnel security procedures.

PS-2, POSITION RISK DESIGNATION:

- The organization assigns a risk designation to all organizational positions, establishes screening criteria for individuals filling those positions, and reviews and updates position risk designations.

PS-3, PERSONNEL SCREENING:

- The organization screens individuals prior to authorizing access to the information system, and rescreens individuals periodically.

...NIST 800-53: Personnel Security (PS)...

PS-4, PERSONNEL TERMINATION:

- The organization, upon termination of individual employment:
 - Disables information system access a specified time period.
 - Terminates/revokes any authenticators/credentials associated with the individual.
 - Conducts exit interviews that include a discussion of organization-defined information security topics.
 - Retrieves all security-related organizational information system-related property.
 - Retains access to organizational information and information systems formerly controlled by terminated individual.
 - Notifies Human Resources and other applicable departments or individuals.

PS-5, PERSONNEL TRANSFER:

- The organization reviews and confirms whether an individual needs their current logical and physical information systems when they are reassigned or transferred to other positions within the organization.
- The organization initiates the transfer within a specified time period.
- The organization modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
- The organization notifies Human Resources and other applicable departments or individuals

...NIST 800-53: Personnel Security (PS)...

PS-6, ACCESS AGREEMENTS:

- The organization:
 - Develops and documents access agreements for organizational information systems.
 - Reviews and updates the access agreements [Assignment: organization-defined frequency].
 - Ensures that individuals requiring access to organizational information and information systems:
 - Sign appropriate access agreements prior to being granted access, and
 - Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated

PS-7, THIRD-PARTY PERSONNEL SECURITY:

- The organization:
 - Establishes personnel security requirements including security roles and responsibilities for third-party providers.
 - Requires third-party providers to comply with personnel security policies and procedures established by the organization;
 - Documents personnel security requirements;
 - Requires third-party providers to notify the organization of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within a specified time period, and
 - Monitors provider compliance.

¹ "NIST Special Publication 800-53, Rev 4", National Institute of Standards and Technology (NIST), 22 Jan 2015, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>

...NIST 800-53: Personnel Security (PS)

PS-8, PERSONNEL SANCTIONS:

- The organization:
 - Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures, and
 - Notifies HR or other applicable departments within a specified time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

NIST 800-53: Program Management (PM)...

PM-1, INFORMATION SECURITY PROGRAM PLAN:

- The organization:
 - Develops and disseminates an organization-wide information security program plan that:
 - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.
 - Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
 - Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical).
 - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.
 - Reviews the organization-wide information security program plan periodically.
 - Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments.
 - Protects the information security program plan from unauthorized disclosure and modification.

...NIST 800-53: Program Management (PM)...

PM-2, SENIOR INFORMATION SECURITY OFFICER:

- The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

PM-3, INFORMATION SECURITY RESOURCES:

- The organization:
 - Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.
 - Employs a business case/Exhibit 300/Exhibit 53 to record the resources required.
 - Ensures that information security resources are available for expenditure as planned.

...NIST 800-53: Program Management (PM)...

PM-4, PLAN OF ACTION AND MILESTONES PROCESS:

- The organization:
 - Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
 - Are developed and maintained;
 - Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
 - Are reported in accordance with OMB FISMA reporting requirements.
 - Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PM-5, INFORMATION SYSTEM INVENTORY:

- The organization develops and maintains an inventory of its information systems.

PM-6, INFORMATION SECURITY MEASURES OF PERFORMANCE:

- The organization develops, monitors, and reports on the results of information security measures of performance.

¹ "NIST Special Publication 800-53, Rev 4", National Institute of Standards and Technology (NIST), 22 Jan 2015, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>

...NIST 800-53: Program Management (PM)...

PM-7, ENTERPRISE ARCHITECTURE:

- The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

PM-8, CRITICAL INFRASTRUCTURE PLAN:

- The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

PM-9, RISK MANAGEMENT STRATEGY:

- The organization:
 - Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems.
 - Implements the risk management strategy consistently across the organization.
 - Reviews and updates the risk management strategy periodically or as required, to address organizational changes.

...NIST 800-53: Program Management (PM)

PM-10, SECURITY AUTHORIZATION PROCESS:

- The organization:
 - Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes.
 - Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process.
 - Fully integrates the security authorization processes into an organization-wide risk management program.

¹ "NIST Special Publication 800-53, Rev 4", National Institute of Standards and Technology (NIST), 22 Jan 2015, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>

SECTION V

SAFEGUARDING PRIVACY DATA

ADMINISTRATIVE SAFEGUARDS ¹

Security Management Process:

- Organizations must identify and analyze potential risks to PII and must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
- Security Personnel:
 - Organizations must designate a security official who is responsible for developing and implementing its security policies and procedures.
- Information Access Management:
 - Organizations must implement policies and procedures for authorizing access to PII only when such access is appropriate based on the user or recipient's role (role-based access).
- Workforce Training and Management:
 - Organizations must provide for appropriate authorization and supervision of workforce members who work with PII.
 - They must also train all workforce members regarding security policies and procedures and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.
- Evaluation:
 - A covered entity must perform a periodic assessment of how well its security policies and procedures meet requirements.

¹ “Summary of the HIPAA Privacy Rule”, HHS Office of the Secretary, Office for Civil Rights, 26 Jul 2013, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

PHYSICAL SAFEGUARDS ¹

- Facility Access and Control:
 - Organizations must limit physical access to its facilities while ensuring that authorized access is allowed.
- Workstation and Device Security:
 - Organizations must implement policies and procedures to specify proper use of and access to workstations and electronic media.
 - Organizations also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of PII.

¹ “Summary of the HIPAA Privacy Rule”, HHS Office of the Secretary, Office for Civil Rights, 26 Jul 2013, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

- Access Control:
 - A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic PII
- Audit Controls:
 - Organizations must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use PII.
- Integrity Controls:
 - Organizations must implement policies and procedures to ensure that PII is not improperly altered or destroyed. Electronic measures must be put in place to confirm that PII has not been improperly altered or destroyed.
- Transmission Security:
 - A covered entity must implement technical security measures that guard against unauthorized access to PII that is being transmitted over an electronic network.

¹ “Summary of the HIPAA Privacy Rule”, HHS Office of the Secretary, Office for Civil Rights, 26 Jul 2013, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

SECTION VI

SECURITY BREACH AND DATA LOSS INCIDENT REPORTING PROCEDURES

SECURITY BREACH AGREEMENT

The “Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration” and other agreements provide procedures and guidelines for preventing, detecting and reporting security breach incidents. ¹

¹ “2019 Medi-Cal PSA Exhibit A, Attachment 4, Electronic Information Exchange Security Requirements and Procedures (Technical Systems Security Requirements – TSSR)”

PRIVACY BREACH DEFINITION

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where

- (1) a person other than an authorized user accesses or potentially accesses data or
- (2) an authorized user accesses data for an other than authorized purpose. ¹

¹"NIST Privacy Framework: An Enterprise Risk Management Tool", NIST.GOV, 30-Apr-2019, <https://www.nist.gov/system/files/documents/2019/04/30/nist-privacy-framework-discussion-draft.pdf>

- External Threat:

- Cyber attacks have increased in frequency and sophistication, presenting significant challenges for organizations that must defend their data and systems from capable threat actors. These actors range from individual, autonomous attackers to well-resourced groups operating in a coordinated manner as part of a criminal enterprise or on behalf of a nation-state. Threat actors can be persistent, motivated, and agile, and they use a variety of tactics, techniques, and procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, and expose or steal intellectual property and other sensitive information.¹

- Insider Threat:

- The Department of Homeland Security National Cybersecurity and Communications Integration Center advises that “insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices.” Threats can also result from employee carelessness or policy violations that allow system access to malicious outsiders. These activities typically persist over time, and occur in all types of work environments, ranging from private companies to government agencies.²

- Medical Data Breaches:

- A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment³.

¹ “NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing”, October 2016, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>

² “Insider Threat - Cyber”, CISA, Cybersecurity & Infrastructure Security Agency, 3 March 2019, <https://www.cisa.gov/insider-threat-cyber>

³ “Breach Notification Rule”, HHS Breach Notification Rule, 26 July 2013, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

SECTION VII

THREATS TO ACCESS CONTROL

Countermeasures for Mobile Applications

- Meeting mobile security standards
- Tailoring security audits to assess mobile application vulnerabilities
- Secure provisioning
- Control and monitoring of application data on personal devices

Countermeasures for Web 2.0

- Security API
- CAPTCHA
- Unique security tokens
- Transactional approval workflows

Countermeasures for Cloud Computing Services

- Cloud computing security assessment
- Compliance-audit assessment on cloud computing providers
- Due diligence
- Encryption in transit and at rest
- Monitoring

BRUTE-FORCE ATTACKS

Brute-force attacks occur when the attacker attempts to determine an encryption key or a user's password by (theoretically) trying every possible combination.

When attempting to discover an encryption key, brute-force means trying all possible keys until one is found that decrypts the ciphertext (encrypted data). This is why key length is such an important factor in cryptosystem strength. ¹

Brute-force password attacks consist of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. ²

¹ Gordon, A. (2015). Official (ISC)2 Guide to the CISSP CBK (4th ed.). Boca Raton, FL: CRC Press, Taylor & Francis Group.

² "Brute-force Attack", Open Web Application Security Project (OWASP), https://owasp.org/www-community/attacks/Brute_force_attack

Email Spoofing – usually used to execute phishing attacks (see below) - occurs when an email is sent that appears to be from a legitimate sender, but is in fact from a spammer. The most effective protection against spoofing (besides the many system tools we employ) is for you to determine whether the suspected email is plausible coming from the sender or not ¹. You’ve probably seen odd emails from people you know, with links to unknown websites, etc. These are likely spoofed emails.

If you receive such an email, please forward to the Security Team with a subject of “possible spoofing” and then permanently delete it immediately.

¹ Gordon, A. (2015). Official (ISC)2 Guide to the CISSP CBK (4th ed.). Boca Raton, FL: CRC Press, Taylor & Francis Group

Phishing is a scam in which the perpetrator sends out legitimate-looking e-mails (often from spoofed email addresses), in an effort to phish (pronounced “fish”) for personal and financial information from the recipient ¹. Often, these emails try to get you to click malicious links by purporting that they need your login credentials, or that they attempted to deliver a package to your house, that you are owed money, that your Netflix account is locked etc. Clicking the links can sometimes install malicious software. Other times, the links take you to legitimate-looking pages that ask you to enter your username and password but collect those credentials for future use.

For more examples of phishing scams and ways to identify them, see <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>.

Again, your diligence is the most effective defense against phishing. No email should ever request credentials. Be wary of ever clicking any links in emails unless you are 100% certain they are legitimate. Often – as in the case of the Netflix scam - the text of the links may look legitimate (such as “Update Account Now”) but hovering over the link reveals that the URL is not from the purported sender at all. If you are unsure, often a simple internet search will reveal the email as a scam. Again, if you receive an email you suspect of being a phishing scam, please forward to the Security Team with a subject of “possible phishing scam”, and then permanently delete it immediately.

¹ Gordon, A. (2015). Official (ISC)2 Guide to the CISSP CBK (4th ed.). Boca Raton, FL: CRC Press, Taylor & Francis Group

Pharming like spoofing occurs when either a legitimate web URL is misdirected to an imposter server's IP address, or when the URL itself is very similar to – but not identical – to a legitimate URL.

In the first case, a virus or malware can modify system files so that the “translation” between the URL and public IP address (ex: www.CalSAWS.org) does not point to the actual CalSaws.org server, but rather directs you to a malicious server.

In the second case, scammers may send you emails – or point to websites – with URL's that look legitimate, but direct you to imposter websites. This is sometimes accomplished by using symbols that look like normal letters.

Once again, besides many system tools we have implemented, your diligence is critical to defend against pharming attacks. Hovering over links before clicking, determining whether emails and websites appear to be authentic, and only clicking links after you are certain of their authenticity: these are your most valuable tools.

If you suspect a case of pharming, please email the Security Team with a subject of “possible pharming scam”. If the URL was included in an email, please forward the email and then permanently delete it. If the URL exists in a web page, please include the URL of the web page.

IMPORTANT TIPS WHEN TELEWORKING

- Only use authorized computers for remote work.
- Do not share or disclose confidential information, personal information, or sensitive information or data to anyone who is not authorized to view or access the information.
- Do not share your computer with anyone not authorized to perform work for any reason.
- Personnel who work remotely must maintain the same level of security and confidentiality as the CalSAWS workplace.

SECTION VIII

SANCTIONS POLICY FOR PRIVACY AND SECURITY VIOLATIONS

SANCTIONS FOR PRIVACY AND SECURITY VIOLATIONS

Consortium employees, contractors and agents who access, use or disclose SSA, PI or PII data in a manner or purpose not authorized maybe subject to civil and criminal sanctions pursuant to applicable Federal statues.

Policy Statement (Sanctions Policy for Privacy and Security Violations)

Consortium employees, vendors, contractors and agents must protect CalSAWS data from all known security and privacy risks which include unauthorized access, use, disclosure, modification, destruction, and removal.

All forms of data are covered by this policy, including but not limited to paper, any systems used to capture electronic data, as well as any media used for creating, obtaining or capturing data.

ACKNOWLEDGEMENT OF TRAINING AND UNDERSTANDING

Please visit the website below to begin the review of material. You will be presented with multiple choice questions to confirm your understanding of this training and will be able to download your training certificate.

<https://placeholder-for-calsaws-url.com>

You may use this presentation while reviewing the training.

For questions or concerns regarding this training please email Consortium.Tech.Security@CalSAWS.org

PERSONAL INFORMATION (PI)

Some sources state that Personal Information, or PI is synonymous with PII. But a new California law (California Consumer Privacy Act ¹) broadens the scope of personal information by identifying Personal Information as: *Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.*

¹ "California Consumer Privacy Act", Wikipedia, Wikimedia Foundation, 1 Jan 2020, https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally identifiable information, or PII, is any data that could potentially be used to identify a particular person. Examples include a full name, Social Security number, driver's license number, bank account number, passport number, and email address.

GLOSSARY OF TERMS

- CalSAWS Consortium: California Statewide Automated Welfare System Joint Powers Authority
- CalSAWS: California Statewide Automated Welfare System
- CDSS: California Department of Social Services
- CMA: Computer Matching Agreement
- Data: A piece of information
- DHCS: California Department of Health Care Services
- DHS: Department of Homeland Security
- EDD: Employment Development Department
- EIEP: Electronic Information Exchange Partner
- EIES: Electronic Information Exchange Security
- Flow Down Regulations: Regulations mandated by PSAs
- HIPAA: Health Insurance Portability and Accountability Act
- IEA: Information Exchange Agreement
- IEVS: Income and Eligibility Verification System
- Information: Data that is accurate, specific and organized for a purpose and presented within a context that gives it meaning and relevance
- LEADER: Los Angeles Eligibility, Automated Determination, Evaluation, and Reporting System
- LRS: LEADER Replacement System
- MEDS: Medi-Cal Eligibility Data System
- PHI: Protected Health Information
- PI: Personal Information
- PII: Personally Identifiable Information
- PSA: Privacy and Security Agreement
- Sanctions: Penalty, punishment, deterrent; punitive action, discipline
- SAVE: Systematic Alien Verification for Entitlements (Program)
- SDI: State Disability Insurance
- SNAP: Supplemental Nutrition Assistance Program
- SSA: Social Security Administration
- SSN: Social Security Number
- TANF: Temporary Assistance to Needy Families
- UI: Unemployment Insurance
- Workforce Individual: A person in the workforce
- Workforce: Consortium employees, vendors, contractors and sub-contractors